Sesión Especial 7

Sesión especial de la red MATSI: Criptografia

Organizadores:

- Verónica Requena (Universidad de Alicante)
- Miguel Beltrá (Universidad de Alicante)
- Sara Díaz Cardell (Universidade Estadual Paulista)

Descripción:
La teoría de la información fue introducida por Claude Shannon y Warren Weaver a finales de los años 40. Corresponde a una rama de las matemáticas y de la computación que estudia la transmisión y el procesamiento de datos. La criptografía es un método de protección de la información y las comunicaciones; además de una herramienta fundamental en la protección de la privacidad y la seguridad en la era digital, y su relación con las matemáticas es crucial. El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográcos para dotar de alguna forma de seguridad. La combinación de criptografía y tecnología proporciona la base para una infraestructura digital segura y eciente en esta era digital. En esta sesión pretendemos recoger distintas nociones, métodos y algoritmos propios del álgebra, la geometría, la combinatoria, la estadística y la computación, que están siendo desarrolladas por diferentes investigadoras e investigadores españoles, atendiendo al área de la criptografía y sus variantes.

Programa

LUNES, 22 de enero:

16:00 – 16:30	Domingo Gómez Pérez (Universidad de Cantabria) *Complexity measures of Interleaved sequences*
16:30 – 17:00	María Isabel González Vasco (Universidad Rey Juan Carlos) *Q-Alice y C-Bob tienen que hablar*
17:00 – 17:30	José Andrés Armario Sampalo (Universidad de Sevilla) *On self-dual Butson bent sequences*

MARTES, 23 de enero:

11:30 – 12:00	Amparo Fúster-Sabater (C.S.I.C) *ASCON: el nuevo estándar de Criptografía ligera*
12:00 – 12:30	Luis Hernández (C.S.I.C) *Futuros Estándares de la Criptografía Postcuántica*
12:30 – 13:00	Agustín Martín (C.S.I.C) *Seguridad de las implementaciones de los algoritmos Criptográficos*
13:00 – 13:30	Daniel Sadornil (Universidad de Cantabria) *Medidas de aleatoriedad de secuencias*
16:00 – 16:30	Josep Miret (Universidad de Lleida) *Alicia en el mundo supersingular*
16:30 – 17:00	Oriol Farrás (Universitat Rovira i Virgili) *Recent Advances in Secret Sharing Schemes for General Access Structures*
17:00 – 17:30	Miguel Beltrá (Universidad de Alicante) *Criptosistema de McEliece con códigos convolucionales y secuencias truncadas*

Complexity measures of Interleaved sequences

D. Gómez-Pérez, J. M. Prellezo

Dpto. de Matemáticas, Estadística y Computación, Universidad de Cantabria

domingo.gomez@unican.es

Abstract: Pseudorandom binary sequences are sequences of zeros and ones that generated by deterministic algorithms. They are not random at all, but they should not be distinguishable from a 'truly' random sequence. Although that there are many constructions, they all rely on conjectures on the computational complexity of a problem. A standard procedure to validate unconditionally the quality of a construction of binary sequences relies on testing on them predictors, i.e. efficient algorithms that from an small portion of the sequence can predict the rest of it.
The main objective of this talk is to detect non random behaviour in binary sequences with interleave structure by studying pseudorandom measurements, like linear complexity, maximum order complexity, 2-adic complexity, etc [2, 3]. For that task, we extend previous results about non randomness of interleave sequences [1].

Referencias

[1] A. I. Gómez, D. Gomez-Perez, A. Tirkel (2023). Correlation Measure of Binary Sequence Families With Trace Representation. Arithmetic of Finite Fields. WAIFI 2022. Lecture Notes in Computer Science, vol 13638.

[2] L. Mérai, H. Niederreiter, A. Winterhof (2017). Expansion complexity and linear complexity of sequences over finite fields. Cryptography and Communications 9.4, 501-509.

[3] A. Winterhof (2023). Pseudorandom binary sequences: quality measures and number-theoretic constructions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.

Q-Alice y C-Bob tienen que hablar

M.I. González Vasco, R. Steinwandt

Departamento de Matemáticas, Universidad Carlos III de Madrid

mariaisabel.gonzalez@uc3m.es

Resumen: Los avances en computación cuántica han motivado el desarrollo de numerosas herramientas criptográficas potencialmente robustas ante ataques implementados con hardware cuántico. Estas herramientas, llamadas *post-cuánticas*, se implementan a través de tecnología *clásica* (es decir, se asume que los usuarios legítimos son máquinas de Turing probabilísticas) y su seguridad se demuestra usando modelos de seguridad habituales. En el caso de esquemas de intercambio de clave para dos usuarios, los modelos establecidos (e.g., [1]) no son útiles para analizar la seguridad de herramientas que usan tecnología cuántica, los llamados esquemas QKD (de Quantum Key Distribution), cuya seguridad puede analizarse usando el modelo de Mosca y otros propuesto en [2]. Pero, ¿qué ocurre cuando el intercambio de clave involucra a más de dos usuarios, y algunos de éstos utilizan a tal fin tecnología cuántica, siendo otros esencialmente *clásicos*? En esta charla presentaremos los retos formales a los que nos enfrentamos para evaluar este tipo de construcciones, y comentaremos el tipo de soluciones que estamos desarrollando en el marco de un proyecto financiado por el programa *Science for Peace and Security* de la OTAN.

Referencias

[1] R. Canetti, H. Krawczyk, B. Pfitzmann (2001). Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, Proceedings of Eurocrypt 2001, Springer, LNCS, Vol. 2045 pp. 453 –474.

[2] M. Mosca, D. Stebila, B. UStaoglu (2013). Quantum Key Distribution in the Classical Authenticated Key Exchange Framework, Proceedings of Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Springer, LNCS, Vol. 7932, pp. 136–154.

Agradecimientos: Este trabajo está financiado por los proyectos CREEME (MINECO PID2019-109379RB-I00) y Secure Communication via Classical and Quantum Technologies, (NATO SPS Project G5985)

On self-dual Butson bent sequences

José Andrés Armario

Departamento de Matemática Aplicada I, Universidad de Sevilla

armario@us.es

Abstract: A new notion of bent sequences, motivated by a cryptographic problem (PUFs=Physically Unclonable Functions), was introduced in [2] as a solution in X, Y to the system

$$\frac{1}{\sqrt{n}} HX = Y,$$

where H is a real Hadamard matrix of order n and $X, Y \in \{\pm 1\}^n$. X is called *a bent sequence for* H. If H is the Sylvester Hadamard matrix then any bent Boolean function $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ determines a bent sequence for H by the rule $X = (-1)^f$ (and vice versa).
In this talk, we deal with the problem of extending the notion of self-dual bent sequences for Butson Hadamard matrices and we will review some of the recent progresses on this topic [1, 3].

Referencias

[1] J.A. Armario, R. Egan, P. Ó Catháin (2023). On the matrix equation $MX = \overline{X}$ and self-dual Butson bent sequences. The 8th International Workshop on Boolean Functions and their Applications, Voss, Norway, Sep 3–8, https://boolean.w.uib.no/bfa-2023/

[2] P. Solé, W. Cheng, S. Guilley, and O. Rioul (2021). Bent sequences over Hadamard codes for physically unclonable functions, IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, 801-806.

[3] M. Shi, D. Lu, J.A. Armario, R. Egan, F. Ozbudak, and P. Solé (2023). Butson Hadamard matrices, bent sequences, and spherical codes. Submitted.

Acknowledgments: This research was partially supported by the Strategic R+D Project TED2021-130566B-I00 from the Ministry of Science and Innovation of the Government of Spain.

ASCON: el nuevo estándar de Criptografía ligera

A. Fúster Sabater, S. Díaz Cardell, V. Requena Arévalo

Instituto de Tecnologías Físicas y de la Información, CSIC, Madrid.

amparo.fuster@csic.es

Resumen: ASCON cipher suite es un criptosistema que unifica en un solo algoritmo los procesos de Autenticación, Cifrado y Manejo de Datos Asociados (esquema AEAD: Authentication Encryption and Associated Data). Se trata de un criptosistema ligero y de fácil implementación, por tanto muy adecuado para comunicaciones entre dispositivos con poca capacidad y escasos recursos computacionales, por ejemplo en IoT. ASCON ha sido recientemente seleccionado por el NIST (National Institute of Standards and Technology) como estándar de Criptografía ligera en la convocatoria *NIST Lightweight Cryptography Competition* (2019 - 2023) [1]. Previamente había sido seleccionado como primera elección en el portfolio final de la convocatoria *CAESAR Competition* (2014 - 2019) [2]. En este trabajo se describe y analiza el criptosistema ASCON y sus variantes, ASCON-128, ASCON-128a y ASCON-80pq. Se evaluan los margenes de seguridad aceptados a día de hoy, a la vez que se introduce un análisis de pseudoaleatoriedad de las secuencias generadas por ASCON en los procesos de cifrado y descifrado.

Referencias

[1] NIST Lightweight Cryptography Standardization project, 2023. https://csrc.nist.gov/projects/lightweight-cryptography/finalists

[2] Final Portfolio, Caesar Competition, 2019. https://competitions.cr.yp.to/caesar.html

Agradecimientos:
Esta publicación es parte del proyecto de I+D+i P2QProMeTe (PID2020-112586RB-I00), financiado por MCIN/AEI/10.13039/501100011033. Asimismo, se ha realizado en el marco de la Red Temática Retos de la Seguridad en Entornos Biomédicos (D5-2022_04) financiada por la Universidad de Málaga.

Futuros Estándares de la Criptografía Postcuántica

Luis Hernández Encinas

Departamento Tecnologías de la Información y las Comunicaciones (TIC)
Consejo Superior de Investigaciones Científicas (CSIC)

luis.h.encinas@csic.es

Resumen: En 1997, P. Shor publicó [1] sendos algoritmos cuánticos capaces de resolver, en tiempo polinómico (una vez que se disponga de ordenadores cuánticos con la suficiente capacidad de cómputo), los dos problemas matemáticos más importantes de la criptografía asimétrica: el problema de la factorización de números enteros y el problema del logaritmo discreto. El primero es la base de la seguridad del RSA y el segundo de los criptosistemas basados en curvas elípticas [2]. Como la criptografía asimétrica actual tiene sus días contados, el NIST (*National Institute of Standards and Technology*) lanzó, en 2016, una Convocatoria Internacional para seleccionar nuevos algoritmos criptográficos resistentes a la computación cuántica, con el fin de ser los nuevos estándares [3]. Esta convocatoria solo considera los mecanismos de encapsulamiento de claves o KEM (*Key Encapsulation Mechanism*) y las firmas digitales. En esta charla se presentarán las principales propuestas de esta convocatoria y los problemas matemáticos en los que basan su seguridad, destacando los considerados como estándares como KEM y firmas digitales, ya publicados como *borradores*.

Referencias

[1] P.W. Shor (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509.

[2] A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini, J. Muñoz Masqué (2012). Criptografía, protección de datos y aplicaciones. RA-MA

[3] NIST (2022). Post-quantum cryptography. Selected algorithms. `https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022`

Agradecimientos: Este trabajo ha sido parcialmente financiado por la Agencia Estatal de Investigación (AEI) del Ministerio de Ciencia e Innovación (MCIN) a través del proyecto P2QProMeTe (PID2020-112586RBI00/AEI/10.13039/501100011033) y por el proyecto QURSA (TED2021-130369BC33), financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea "NextGenerationEU"/PRTR.

Seguridad de las implementaciones de los algoritmos criptográficos

Agustín Martín Muñoz, Alberto Peinado Domínguez

Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)

agustin.martin@csic.es

Resumen: Tradicionalmente los algoritmos criptográficos se diseñaban teniendo en cuenta su seguridad desde un punto de vista matemático. También los diferentes métodos de criptoanálisis se basaban en técnicas matemáticas. Como es sabido, eso cambió cuando en [1] se presentó un ataque basado en el análisis del tiempo de ejecución de las implementaciones de varios criptosistemas asimétricos en dispositivos físicos.
En esta comunicación se describirán los principales métodos (generalmente conocidos como *ataques por canal lateral* [2]) para atacar la seguridad de las implementaciones de los algoritmos criptográficos empleados hoy en día en multitud de dispositivos como tarjetas inteligentes, teléfonos móviles o dispositivos biomédicos [3]. Se explicarán también algunas de las contramedidas que se diseñan para evitar dichos ataques.

Referencias

[1] P. Kocher (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of Advances in Cryptology – CRYPTO'96, LNCS 1109, 104–113.

[2] M. Ouladj, S. Guilley (2021). Side-Channel Analysis of Embedded Systems. An Efficient Algorithmic Approach. Springer.

[3] S. Faezi, S. R. Chhetri, A. V. Malawade, J. C. Chaput, W. H. Grover, P. Brisk, M. A. Al Faruque (2019). Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines. Proceedings of the 26^{th} Annual Network and Distributed System Security Symposium, NDSS.

Agradecimientos: Este trabajo ha sido parcialmente financiado por la Agencia Estatal de Investigación (AEI) del Ministerio de Ciencia e Innovación (MCIN) a través del proyecto P2QProMeTe (PID2020-112586RB-I00/AEI/10.13039/501100011033), y por la Universidad de Málaga a través de la Red temática BIOMED-Sec "Retos de la seguridad en entornos biomédicos" (referencia D5-2022-04).

Medidas de aleatoriedad de secuencias

D. Sadornil, D. Gómez-Pérez

Dpto. de Matemáticas, Estadística y Computación, Universidad de Cantabria

daniel.sadornil@unican.es

Resumen: En el campo de la computación y la estadística, los generadores de números pseudoaleatorios (PRNGs) juegan un papel fundamental en diversas aplicaciones, desde simulaciones hasta criptografía. Aunque estos algoritmos proporcionan secuencias de números aparentemente aleatorios, es esencial someterlos a rigurosos tests de aleatoriedad para garantizar su idoneidad en aplicaciones críticas.
Las secuencias automáticas, dentro de las que incluyen la secuencia Thue-Morse y la secuencia Rudin-Shapiro, han sido ampliamente estudiadas debido a sus propiedades como generadores pseudoaleatorios de números [1], pero además para también han sido utilizados para definir nuevas medidas de aleatoriedad [2].
Recientemente, Arne Winterhof [3] ha recopilado varias preguntas abiertas respecto a subsecuencias de secuencias automáticas y varias de medidas de aleatoriedad como el máximo orden de estas secuencias, la complejidad lineal, etc.
En este charla daremos nuevos resultados de diferentes medidas para estas secuencias y compararemos con los resultados computacionales.

Referencias

[1] J. P. Allouche, J. Shallit (2003). Automatic Sequences: Theory, Applications, Generalizations. Cambridge: Cambridge University Press.

[2] L. Mérai, H. Niederreiter, A. Winterhof (2017). Expansion complexity and linear complexity of sequences over finite fields. Cryptography and Communications 9.4, 501-509.

[3] A. Winterhof (2023). Pseudorandom binary sequences: quality measures and number-theoretic constructions. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences.

Alicia en un mundo supersingular

Josep M. Miret, Jordi Pujolàs, Juan Tena, Javier Valera

Departament de Matemàtica, Universitat de Lleida

josepmaria.miret@udl.cat

Resumen: En estas últimas décadas han aparecido distintos esquemas criptográficos basados en isogenias de curvas elípticas supersingulares, como el intercambio de claves de De Feo-Jao-Plût [3], el de funciones Hash Charles-Goren-Lauter [2] o el esquema de firma Galbraith-Petit-Silva [4]. La seguridad de estos esquemas se basa en la dificultad computacional de encontrar un camino entre dos curvas del grafo supersingular.
En esta charla, haremos un recorrido por algunos de estos protocolos criptográficos, describiendo ciertos aspectos de la estructura de estos grafos de isogenias de curvas elípticas supersingulares [1] en contraste con los grafos de curvas ordinarias [5].

Referencias

[1] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, J. Sotáková (2023). Adventures in supersingularland. Experimental Mathematics. 32(2), 241-268.

[2] D.X. Charles, E.Z. Goren, K.E. Lauter (2009). Cryptographic Hash Functions from Expander Graphs. Journal of Cryptology, 22(1), 93-113.

[3] L. De Feo, D. Jao, J. Plût (2014). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), 209-247.

[4] S. Galbraith, C. Petit, J. Silva (2017). Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. ASIACRYPT 2017, Part I, LNCS 10624, 3-33.

[5] J. Miret, R. Moreno, D. Sadornil, J. Tena, M. Valls (2008). Computing the height of volcanoes of ℓ-isogenies of elliptic curves over finite fields. Applied mathematics and computation, 196(1), 67-76.

Agradecimientos: Trabajo financiado por el Ministerio de Ciencia e Innovación mediante el proyecto PID2021-124613OB-I00, por la Generalitat de Catalunya mediante el grupo 2021SGR 00434 y por la red Iberoamerica 522RT0131 de CyTeD.

Recent Advances in Secret Sharing Schemes for General Access Structures

Oriol Farràs

Departament d'Enginyeria Informàtica i Matemàtiques, Universitat Rovira i Virgili

oriol.farras@urv.cat

Abstract: A secret sharing scheme is a method by which a dealer distributes shares to parties such that only authorized subsets of parties can reconstruct the secret. The family of these authorized subsets is called the access structure of the scheme.
The share size of secret sharing schemes for general access structures is poorly understood. The gap between the best known upper bound on the total share size per party of $1{,}5^n$ [1] and the best known lower bound of $\Omega(n/\log n)$ [4] is huge (where n is the number of parties in the scheme).
This talk is dedicated to the latest constructions for general access structures. In particular, we will review a joint work with Amos Beimel and Or Lasri [3] dedicated to polinomial secret sharing schemes.

Referencias

[1] B. Applebaum, O. Nir (2021). Upslices, downslices, and secret-sharing with complexity of $1{,}5^n$. CRYPTO 2021, volume 12827 of LNCS, pages 627–655. Springer-Verlag.

[2] A. Beimel, O. Farràs (2020). The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs. Theory of Cryptography, TCC 2020, volume 12552 of LNCS, pages 499–529.

[3] A. Beimel, O. Farràs, O. Lasri (2023). Improved Polynomial Secret-Sharing Schemes. To appear in Theory of Cryptography, TCC.

[4] L. Csirmaz (1997). The size of a share must be large. J. of Cryptology, 10(4):223–231.

Criptosistema de McEliece con códigos convolucionales y secuencias truncadas

Miguel Beltrá, Paulo Almeida, Diego Napp, Cláudia Sebastião
Departamento de Matemáticas, Universidad de Alicante
miguel.beltra@ua.es

Resumen: El NIST ha llevado a cabo en los últimos años un proceso de estandarización de sistemas de cifrado resistentes a ataques con computadores cuánticos. Entre los candidatos encontramos propuestas basadas en teoría de códigos: *McEliece clásico* [2], *BIKE* y *HQC*. El criptosistema de McEliece fue uno de los primeros criptosistemas propuestos [1]. Basa su seguridad en la dificultad de decodificar un código lineal en general. La propuesta original utiliza códigos binarios de Goppa, que poseen un algoritmo de decodificación eficiente, pero debido a su baja capacidad correctora, es necesario utilizar claves públicas muy grandes para alcanzar los requerimientos de seguridad. Por este motivo el criptosistema nunca se ha utilizado en la práctica.

En esta charla se presentará una variante del criptosistema de McEliece que utiliza códigos de Reed-Solomon con una máscara convolucional [3] que es capaz de reducir considerablemente el tamaño de la clave pública del criptosistema de McEliece.

Referencias

[1] R. J. McEliece. (1978) A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report, 44:114–116.

[2] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Mizoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wen. (2022) Classic McEliece: conservative code-based cryptography. Round 4 submission to the NIST post-quantum cryptography call

[3] P. Almeida, M. Beltrá, D. Napp, and C. Sebastião. (2023) Smaller keys for the mceliece cryptosystem: A convolutional variant with GRS codes. Sumitted.

Agradecimientos: El primer autor y la cuarta autora han sido financiados por el *Centro de Investigação e Desenvolvimento em Matemática e Aplicações* (CIDMA) a través de la *Fundacão para a Ciência e Tecnologia*(FCT), referencia UIDB/04106/2020. El segundo y el tercer autor han sido financiados con el Proyecto Español de I+D+i PID2022-142159OB-I00.